IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEIZURE OF SUMS OF BTC AND USDT STORED IN OR ACCESSIBLE AT BINANCE CRYPTOCURRENCY EXCHANGE ACCOUNTS ASSOCIATED WITH USER IDS 355266437, 282843618, AND 255304050.	Case No. 22-mj-60-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, George Jasek III, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service and have been so employed since March 5, 2018. I am currently assigned to the Manchester, New Hampshire Resident Office. In preparation for my employment with the United States Secret Service I completed the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center in Glynco, Georgia. Additionally, I completed the Special Agent Training Course (SATC) at the United States Secret Service James J. Rowley Training Center in Laurel, Maryland. While attending SATC I received a five-day training titled "Basic Investigation of Computer and Electronic Crimes Program" (BICEP). In addition to these training programs, I have completed numerous in-service training courses related to constitutional law. Prior to my employment with the United States Secret Service, I was a full-time certified Police Officer in Nashua, New Hampshire for over five years. My present duties include the investigation of federal offenses, including, but not limited to, those involving financial fraud and its related activities.

2. As part of my duties I have conducted financial crimes and financial fraud investigations. These investigations have included but are not limited to federal violations of Wire Fraud, Bank

Fraud, Access Device Fraud, Money Laundering, and Identity Theft. During the course of these investigations, I have conferred with other investigators who specialize in computer forensics and who have conducted investigations regarding financial fraud crimes. I have additionally received training regarding computers that includes Basic Network Intrusion Responder Training, Incident Response Analysis, and Cryptocurrency training.

3. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses. This affidavit is intended to show only there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROPERTY TO BE SEIZED

4. This affidavit is made to obtain a seizure warrant for all assets, virtual currency, funds, monies, and other things of value up to the equivalent of 8.47176011 Bitcoin (BTC) ("SUBJECT ASSETS") stored in or accessible at Binance Capital Management Co., Ltd. ("BINANCE") bearing the following User ID(s):

- 1.00176011 Bitcoin ("BTC") stored in or accessible at Binance in an account with a user ID of 355266437 in the name of Harish GIRI (hereinafter referred to as "TARGET BINANCE ACCOUNT 1").
- $9,555.80 Tether ("USDT") stored in or accessible at Binance in an account with a User ID of 282843618 in the name of Deepak SONI (hereinafter referred to as "TARGET BINANCE ACCOUNT 2").

- 6.77 Bitcoin ("BTC") stored in or accessible at Binance in an account with a User ID of 255304050 in the name of Gaurav Garg Suresh GARG (hereinafter referred to as "TARGET BINANCE ACCOUNT 3").

LEGAL AUTHORITY FOR SEIZURE

5. I have probable cause to believe that this property is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) (civil forfeiture) and the same statute as incorporated by 28 U.S.C. § 2461(c) (criminal forfeiture) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 (Wire Fraud) or a conspiracy to commit such offense.

6. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud) or a conspiracy to commit such is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

7. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept. The statute does not, however, allow the government to reach back in time for an unlimited period. A forfeiture action (including a seizure) against property not directly traceable to the offense that is the basis for the forfeiture cannot be commenced more than one year from the date of the offense.

8. I know that once U.S. Currency is converted to cryptocurrency, the funds become difficult to recover and trace. A restraining order would be inadequate to preserve property of this type for forfeiture at trial. Based on my training and experience, I know that restraining orders served on banks sometimes fail to preserve the property for forfeiture because the bank representative receiving the restraining order fails to put the necessary safeguards in place to freeze the money in

time to prevent the account holder from accessing the funds electronically, or fails to notify the proper personnel as to the existence of the order. The risk of such problems is higher, not lower, with virtual currency. In contrast, a seizure warrant guarantees that the funds will be in the government's custody upon execution of the warrant and, thus, preserved for forfeiture.

9. The Court has the authority to issue seizure warrants for assets located in a foreign jurisdiction pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that a seizure warrant may be issued by a "judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)], and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement." 18 U.S.C. § 981(b)(3). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located in a foreign jurisdiction. [1]

FACTS SUPPORTING PROBABLE CAUSE

Investigation Background

10. On or about March 22, 2022 Police Officer Nicholas Powden of the Salem New Hampshire Police Department responded to 3 Artisan Drive Apartment #506, Salem, New Hampshire 03079 where he met with "J.F." regarding the report of a fraud. J.F. reported to Officer Powden that on or about January 11, 2022 J.F. received a fraud alert on her computer which advised her to contact

1 Binance Holdings Limited ("Binance") claims that it is a non-U.S. Company and, therefore, is not subject to U.S. jurisdiction and cannot be compelled by U.S. proceess. Binance has further indicated, however, that it is willing to volutarily freeze the SUBJECT ACCOUNTS, and transfer cryptocurrency to the United States with a seizure warrant issued by a United States Magistrate Judge.

Microsoft. J.F. reported to Officer Powden that after she called the provided number, she was contacted via phone by an individual who identified himself as Litigation Officer Freddie Sandler of the Federal Trade Commission. J.F. told Officer Powden that over a period of approximately two months, the individual known to her as Freddie Sandler provided her with what she believed to be financial advice to protect her assets from fraud. J.F. reported to Officer Powden that the advice included instructions to make wire transfers of large quantities of money from her bank accounts. J.F. reported to Officer Powden that she followed the advice and responded to Chase Bank in Salem, New Hampshire on multiple occasions to complete wire transfers. J.F. provided Officer Powden bank statements showing transaction histories which confirmed multiple wire transfers.

11. On or about March 24, 2022, I was contacted by Detective Josh Dempsey of the Salem New Hampshire Police Department regarding this matter. Detective Dempsey provided an overview as well as a copy of the associated police report…

12. On or about March 25, 2022, I spoke with J.F. regarding this matter who provided further documentation directly to me about the wire transactions she had conducted. J.F. advised that her husband passed away a year and a half ago and that she profited approximately $900,000 on the sale of her home in Osterville, Massachusetts. J.F. said that she had conducted several wire transfers to what she was told to be a "Coinbase cryptocurrency account" and was completed at the direction of Litigation Officer Freddie Sandler. From my training and experience I know that "Coinbase" or Coinbase, Inc. is an American company that operates a cryptocurrency exchange platform. J.F. stated that the Coinbase account was created because Litigation Officer Freddie Sandler convinced J.F. that she could invest her money with him at a less expensive rate than if J.F. were to use an investor. J.F. advised that she did not create the Coinbase cryptocurrency

account herself, but that Litigation Officer Freddie Sandler created it for her while she was on the phone and computer with him, asking J.F. for information needed to set up the account. J.F. believed the Coinbase cryptocurrency account was in her name but was not sure as she had never logged into the account. J.F. provided wire information about where she had wired funds from her Chase bank account to Coinbase. J.F. did say that she had been provided with a password from Litigation Officer Freddie Sandler for the Coinbase cryptocurrency account and she attempted to log into the Coinbase account but was unable to do so.

13. Continuing on or about March 25, 2022, J.F. provided me with specific documentation related to wire transactions as well as bank account information. The following is a list of dates and amounts of wire transfers that J.F. initiated from her Chase Bank account (Account number ending -0060) and are shown below in Figure 1:

2/17/2022	$87,000
2/22/2022	$115,000
2/24/2022	$200,000
3/1/2022	$50,000
3/9/2022	$50,250
3/18/2022	$280,000
TOTAL = $782,250	

FIGURE 1

I verified the above listed wire transfers listed in Figure 1 from wire transfer outgoing request documents provided by J.F. for each of the above wires from Chase bank account ending 0060 to the following recipient information:

Recipient Account number: 317590141535

Recipient Bank Information:

Bank Name: Cross River Bank

Street Address: 885 Teaneck Road, Teaneck, New Jersey 07666

Bank ABA / Swift Code: 021214891

The above recipient information was the same for all six wire transfers initiated by J.F.

14. From my training and experience I know that Cross River Bank is partnered with Coinbase to facilitate cryptocurrency transactions. I also know that wire transfers can be conducted to fund cryptocurrency deposits.

15. On or about March 25, 2022, Coinbase was provided with the six wire transfers from J.F.'s Chase Bank account ending 0060 listed in Figure 1 to the above listed recipient information. Coinbase advised that Coinbase account UID 61df4cdbb12d1d185e5d9edd received all of the funds from J.F.'s Chase Bank account ending 0060. Coinbase confirmed that Coinbase UID 61df4cdbb12d1d185e5d9edd account is in the name of J.F. Coinbase was provided with Identification photos and a picture of an individual holding up a sign "for Coinbase trading" in an identification selfie regarding Coinbase UID 61df4cdbb12d1d185e5d9edd. This photo is of J.F. Coinbase then confirmed that the funds were transferred out of Coinbase account UID 61df4cdbb12d1d185e5d9edd shortly thereafter, as outlined in Figure 2 below:

Amount (BTC)	Outgoing Transaction Destination	Date
0.02417368	bc1qss73rcpw7hdhhsk678r93dpvz9mpyrks7e7fep	2/8/2022
2.13081003	bc1qss73rcpw7hdhhsk678r93dpvz9mpyrks7e7fep	2/17/2022
2.99222984	bc1qss73rcpw7hdhhsk678r93dpvz9mpyrks7e7fep	2/22/2022
5.48314555	bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0	2/24/2022
1.1467604	bc1qt306nf8l676wrntq4g3hwmk5q9r869ghmlchs2	3/1/2022
1.16956515	bc1qnma5v0ldew6rh5ty694yfnwlgl8ulh26c558ur	3/9/2022
0.27395586	bc1q2uphy5zdvypvnescjznqmpc9dglyfam927xnaw	3/17/2022
6.69580261	bc1qfxpt6n6gtfqftrupgxrngjg8nfq278lshcdm2g	3/18/2022

FIGURE 2

The total amount of all BTC sent out of Coinbase UID 61df4cdbb12d1d185e5d9edd depicted above in Figure 2 is 19.91644312 BTC. This is consistent with the funds sent from J.F. to Coinbase.

16. On March 30, 2022, Coinbase advised they use a "hot wallet system" which means that funds are intermingled with other customers regarding cryptocurrency transactions. Coinbase advised that no specific address is assigned for outgoing cryptocurrency transactions.

17. On March 30, 2022 I spoke further with J.F. regarding this investigation. J.F. confirmed that she had provided Litigation Officer Freddie Sandler with a "selfie" type photograph of herself for a Coinbase account to be created. J.F. advised that she provided information to Litigation Officer Freddie Sandler to open the Coinbase account such as a code that was texted to her cellular phone during account creation. From my training and experience I know this to be "Multi Factor Authentication" which is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.

18. J.F. further advised that when she received the fraud alert on her computer asking her to contact Microsoft, she contacted a phone number of (813) 303-5827 on January 11, 2022. J.F. said that she received a call back from someone stating they were Litigation Officer Freddie Sandler with the Federal Trade Commission. J.F. said that over the next few months she communicated with Litigation Officer Freddie Sandler via phone number of (425) 645-1715. J.F. stated that Litigation Officer Freddie Sandler was a male who had an accent. J.F. said she spoke on the phone and texted with the previously mentioned phone number on a daily basis. J.F. also stated and provided documentation that she communicated with Litigation Officer Freddie Sandler through an email address of protectionteamfraud@gmail.com. J.F. said that Litigation Officer Freddie

Sandler had provided a United States government identification card and email correspondence with the Federal Trade Commission seal. I viewed a copy of the government identification card provided to J.F. and believe it to be fraudulent.

19. J.F. stated that she had installed an application called "AnyDesk" which J.F. said allowed Litigation Officer Freddie Sandler to see her bank accounts. I am familiar with AnyDesk through my training and experience and know that it is a remote desktop application allowing remote access to personal computers and other devices that are running the application.

20. From my training and experience I am familiar with fraud alerts or technical support scams are common ways of targeting victims which instruct them to contact Microsoft. The victims are not actually contacting Microsoft and in fact contact individuals who will attempt to commit fraud. I am also aware that individuals will purport themselves to be representatives of the United States Government to facilitate fraud.

21. As evidenced by J.F.'s statements and documents provided between on or about February 17, 2022 and on or about March 18, 2022 the individual identifying themselves as Litigation Officer Freddie Sandler with the Federal Trade Commission instructed J.F. to transfer approximately $782,250 to cryptocurrency wallets. Accordingly, I have probable cause to believe J.F. was fraudulently induced to transfer funds to a cryptocurrency platform that J.F. did not control *i.e.* wire fraud in violation of 18 U.S.C. § 1343.

THE FLOW OF FUNDS TO TARGET BINANCE ACCOUNT 1

22. Subsequent analysis indicates that funds in TARGET BINANCE ACCOUNT 1 can be traced to the transfers from Coinbase UID 61df4cdbb12d1d185e5d9edd that was funded by transfers outlined above in Figure 1. These funds were remitted to a series of intermediary wallets before all these funds (1.00176011 BTC) were ultimately transferred to TARGET BINANCE

ACCOUNT 1. Intermediary wallets are typically private wallets or non-exchange wallets that obfuscate transactions on the blockchain. Intermediary wallets support the movement of illicitly obtained funds as they help conceal and disguise the source by layering and severing straight line coordinates of transaction activity on the Blockchain to cash out exchangers.

23. A listing of the transactions to TARGET BINANCE ACCOUNT 1 through intermediary wallets can be found in Figure 3 below, with times shown in UTC: 2.

Date: 2/22/2022 5:44:00 PM
Amount BTC: 2.99222984
Sending Address: bc1q22gaxgvxe5370mqf8jaym2fpx4uj3xe0gxaaak (COINBASE)
Receiving Address: bc1qss73rcpw7hdhhsk678r93dpvz9mpyrks7e7fep
Transaction Hash: bacb8b26a92718a171aac155ad22b55466d80dc5712d8116a5c020c0bba515c0
Date: 3/9/2022 6:47:00 PM
Amount BTC: 1.00176011
Sending Address: bc1qss73rcpw7hdhhsk678r93dpvz9mpyrks7e7fep
Receiving Address: 13x9CCsjsrPMDbxLoqq6M3qN4TT1bumLpz (TARGET BINANCE ACCOUNT 1)
Transaction Hash: 92b8e77759b2400be29f7626ce6de13f45b6d07b334feb69ed4a0ff60e70bf2d

FIGURE 3

A visual depiction containing the transfers listed in Figure 3, are reflected in Attachment A.

24. Binance records indicate that the owner of deposit address 13x9CCsjsrPMDbxLoqq6M3qN4TT1bumLpz is linked to Binance User ID 355266437. Binance records reveal that User ID 355266437 is owned by Harish GIRI. Binance verification records also reveal that GIRI (Date of Birth: October 5, 1989) provided a Government of India identification.

2 UTC is Universal Time Coordinated, also known as Coordinated Universal Time. This is also known as Greenwich Mean Time.

Additionally, IP address login information from Binance corroborate User ID 355266437 is located in India.

25. Binance records reveal that GIRI's Binance account with User ID 355266437 receives a large number of deposits and conducts a large amount of withdrawals from the account. As of March 30, 2022, Binance records reveal that the TARGET BINANCE ACCOUNT 1 held numerous virtual currencies to include, but not limited to, Bitcoin ("BTC") and TetherUS ("USDT"). The total balance as of March 30, 2022, held in TARGET BINANCE ACCOUNT 1 converted to Bitcoin is approximately 2.17789964 BTC.

26. Binance records confirm that Binance account with a User ID 355266437 received a deposit of 1.00176001 BTC outlined in Figure 3 on March 9, 2022. The last withdrawal from Binance account with a User ID 355266437 was completed on March 8, 2022. Therefore, since the funds linked to J.F. have been deposited into the account, there have been no withdrawals. Although the account contains more cryptocurrency (and cryptocurrencies other than bitcoin), I seek only to seize the amount of bitcoin to correspond with the bitcoin transferred from J.F.'s Coinbase account.

THE FLOW OF FUNDS TO TARGET BINANCE ACCOUNT 2

27. Further analysis indicates that the funds in TARGET BINANCE ACCOUNT 2 can be traced to the transfers from Coinbase UID 61df4cdbb12d1d185e5d9edd that was funded by transfers outlined above in Figure 1. These funds were remitted to a series of intermediary wallets before all these funds (0.7 BTC) were ultimately transferred to TARGET BINANCE ACCOUNT 2.

28. A listing of the transactions to TARGET BINANCE ACCOUNT 2 through intermediary wallets can be found in Figure 4 below, with times shown in UTC:

Date: 2/24/2022 5:57:00 PM
Amount BTC: 5.48314555
Sending Address: 3JBHAYb5uRM9BLPoneqSGqk5pe1f7khVPu (COINBASE)
Receiving Address: bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0
Transaction Hash: 0a7896e079d270e3baa9a35d733fea0ae61528f1c14cebeb2edd66aa403dc14f
Date: 2/24/2022 6:38:00 PM
Amount BTC: 4.78314108
Sending Address: bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0
Receiving Address: bc1qyjzapkvs5fyyzpvh7k4krkn5avxhy9kjajte7a
Transaction Hash: 74267712c1c3a4d7525a66682fd2c4ed60bcdaa82d230bfd28f3df8f16ae07c5
Date: 2/24/2022 7:16:00 PM
Amount BTC: 0.7
Sending Address: bc1qyjzapkvs5fyyzpvh7k4krkn5avxhy9kjajte7a
Receiving Address: 1GG4wWsy2Eqy3j4x31eBFdcjEaS8rtnVeG (TARGET BINANCE ACCOUNT 2)
Transaction Hash: 30552056ad1c43e8dc7d1d8648828ca007b624f390245a6308951771d84eb482

FIGURE 4

A visual depiction containing the transfers listed in Figure 4, are reflected in Attachment B.

29. Binance records indicate that the owner of deposit address 1GG4wWsy2Eqy3j4x31eBFdcjEaS8rtnVeG is linked to Binance User ID 282843618. Binance records reveal that User ID 282843618 is owned by Deepak SONI. Binance verification records also reveal that SONI provided a Government of India identification card which lists a year of birth of 1992. Additionally, IP address login information from Binance corroborate that User ID 282843618 is located in India.

30. Binance records reveal that SONI's Binance account with User ID 282843618 receives a large number of deposits, conducts a large number of withdrawals, and conducts a large number of trades. As of March 30, 2022, Binance records reveal that TARGET BINANCE ACCOUNT 2

held numerous virtual currencies to include, but not limited to, Tornado Cash ("TORN"), Bitcoin ("BTC"), Ethereum ("ETH"), TetherUS ("USDT"), Ripple ("XRP"), and Solana ("SOL"). The total balance as of March 30, 2022, held in TARGET BINANCE ACCOUNT 2 converted to Bitcoin is approximately 0.48548116 BTC.

31. Binance records show a 0.7 BTC deposit on February 24, 2022. Less than an hour later, 0.7 BTC was transferred to USDT ("Tether"), leaving $26,600 tether in the account.

32. Since the victim funds were deposited into this account, there were various transfers into and out of this account. The lowest value of the account, on February 24, 2022, was $14,110. The current value of tether in the account is $9,555.80, less than the lowest value of the account. I seek only to seize this amount of Tether.

THE FLOW OF FUNDS TO TARGET BINANCE ACCOUNT 3

33. Further analysis indicates that the funds in TARGET BINANCE ACCOUNT 3 can be traced to the transfers from Coinbase UID 61df4cdbb12d1d185e5d9edd that was funded by transfers outlined above in Figure 1. These funds were remitted to a series of intermediary wallets before all these funds (6.77 BTC) were ultimately transferred to TARGET BINANCE ACCOUNT 3.

34. A listing of the transactions to TARGET BINANCE ACCOUNT 3 of 1.4 BTC through intermediary wallets can be found in Figure 5 below, with times shown in UTC:

Date: 2/24/2022 5:57:00 PM
Amount BTC: 5.48314555
Sending Address: 3JBHAYb5uRM9BLPoneqSGqk5pe1f7khVPu (COINBASE)
Receiving Address: bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0
Transaction Hash: 0a7896e079d270e3baa9a35d733fea0ae61528f1c14cebeb2edd66aa403dc14f
Date: 2/24/2022 6:38:00 PM

Amount BTC: 4.78314108
Sending Address: bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0
Receiving Address: bc1qyjzapkvs5fyyzpvh7k4krkn5avxhy9kjajte7a
Transaction Hash: 74267712c1c3a4d7525a66682fd2c4ed60bcdaa82d230bfd28f3df8f16ae07c5
Date: 2/24/2022 7:16:00 PM
Amount BTC: 4.08313772
Sending Address: bc1qyjzapkvs5fyyzpvh7k4krkn5avxhy9kjajte7a
Receiving Address: bc1q6pfcyxzrypazptwpaz24avtly694r0yev4vaqh
Transaction Hash: 30552056ad1c43e8dc7d1d8648828ca007b624f390245a6308951771d84eb482
Date: 2/24/2022 7:16:00 PM
Amount BTC: 1.38
Sending Address: bc1q6pfcyxzrypazptwpaz24avtly694r0yev4vaqh
Receiving Address: bc1qdk4s5kwh6uslvqy44ajksynjf2c564n6f6x2m3
Transaction Hash: 1b53003d80a13d05d5d09a090318ecb58b485a1ef66ab333764e6ae212e1f119
Date: 2/26/2022 1:10:00 AM
Amount BTC: 1.4
Sending Address: bc1qdk4s5kwh6uslvqy44ajksynjf2c564n6f6x2m3
Receiving Address: 1QJ8Ztg3JTq1Fsi7teU6b7Lr67Fai6Fcxo (TARGET BINANCE ACCOUNT 3)
Transaction Hash: 5c18eb3242b4c5fec3251344d302cb2cc4fd05c156964b562d44b40088aae79c

FIGURE 5

A visual depiction containing the transfers listed in Figure 5, are reflected in Attachment C.

35. A listing of the transactions to TARGET BINANCE ACCOUNT 3 of 5.37 BTC through intermediary wallets can be found in Figure 6 and Figure 7 below, with times shown in UTC

Date: 3/1/2022 4:32:00 PM
Amount BTC: 1.1467604
Sending Address: bc1qtk04f4y0vyt4a2v0unrmn3vlpus0qx6kzyk9kt (COINBASE)
Receiving Cluster: bc1qs5f3ta0rchzelsp5q8ptarr4sy9kfk8fkh36mc
Receiving Address: bc1qt306nf8l676wrntq4g3hwmk5q9r869ghmlchs2
Transaction Hash: 4dd4bb95301d33522e7b618897cc9c5ce88681472954aa51170cde39533abd28

Date: 3/9/2022 9:48:00 PM
Amount BTC: 1.16956515
Sending Address: bc1qk2xsre3dmlq2kfh2l03gqhfeuw6ntvjz83jdq8
Receiving Cluster: bc1qs5f3ta0rchzelsp5q8ptarr4sy9kfk8fkh36mc
Receiving Address: bc1qnma5v0ldew6rh5ty694yfnwlgl8ulh26c558ur
Transaction Hash: 17dfc6fa78e1bebb0d022604c20ddf3d5c5b5767507907b34d77896d76c96e59
Date: 3/18/2022 4:16:00 PM
Amount BTC: 5.3702
Sending Cluster: bc1qs5f3ta0rchzelsp5q8ptarr4sy9kfk8fkh36mc
Receiving Address: bc1qdk4s5kwh6uslvqy44ajksynjf2c564n6f6x2m3
Transaction Hash: 178a968fd048cf2325045a34eac330737d35d60a1effe82ff6f512e0c92f2b35
Date: 3/18/2022 4:26:00 PM
Amount BTC: 5.37
Sending Address: bc1qdk4s5kwh6uslvqy44ajksynjf2c564n6f6x2m3
Receiving Address: 1QJ8Ztg3JTq1Fsi7teU6b7Lr67Fai6Fcxo (TARGET BINANCE ACCOUNT 3)
Transaction Hash: 2a2155d714ee5d1802de62050377374a04b846b29504a7eef7f946b1cf222bcb

FIGURE 6

A visual depiction containing the transfers listed in Figure 6, are reflected in Attachment D.

Date: 2/24/2022 5:57:00 PM
Amount BTC: 5.48314555
Sending Address: 3JBHAYb5uRM9BLPoneqSGqk5pe1f7khVPu (COINBASE)
Receiving Address: bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0
Transaction Hash: 0a7896e079d270e3baa9a35d733fea0ae61528f1c14cebeb2edd66aa403dc14f
Date: 2/24/2022 6:38:00 PM
Amount BTC: 4.78314108
Sending Address: bc1qa4v0t7nt4xw6vhfs5uqhseqh32axfeldn7g4z0
Receiving Address: bc1qyjzapkvs5fyyzpvh7k4krkn5avxhy9kjajte7a

Transaction Hash: 74267712c1c3a4d7525a66682fd2c4ed60bcdaa82d230bfd28f3df8f16ae07c5
Date: 2/24/2022 7:16:00 PM
Amount BTC: 4.08313772
Sending Address: bc1qyjzapkvs5fyyzpvh7k4krkn5avxhy9kjajte7a
Receiving Address: bc1q6pfcyxzrypazptwpaz24avtly694r0yev4vaqh
Transaction Hash: 30552056ad1c43e8dc7d1d8648828ca007b624f390245a6308951771d84eb482
Date: 2/24/2022 7:16:00 PM
Amount BTC: 2.70313337
Sending Address: bc1q6pfcyxzrypazptwpaz24avtly694r0yev4vaqh
Receiving Address: bc1q7nmgvqjv4cpjggl50vs8fy7x0wsk2gd7gfy2xg
Transaction Hash: 1b53003d80a13d05d5d09a090318ecb58b485a1ef66ab333764e6ae212e1f119
Date: 2/25/2022 5:10:00 PM
Amount BTC: 2.54033078
Sending Address: bc1q7nmgvqjv4cpjggl50vs8fy7x0wsk2gd7gfy2xg
Receiving Address: bc1q7dp7d0v7dl8x2dq6r8c30hxz5smphelv67t0cq
Transaction Hash: 2847feacd9d531c9e9a1c65b0bc106963e6c0c4dc3e6c227838003e066fea621
Date: 3/4/2022 6:42:00 AM
Amount BTC: 2.51620984
Sending Address: bc1q7dp7d0v7dl8x2dq6r8c30hxz5smphelv67t0cq
Receiving Cluster: bc1qs5f3ta0rchzelsp5q8ptarr4sy9kfk8fkh36mc
Receiving Address: bc1qv7jguepu4egdld3jpvds9hsnxq33u2f0acg8w6
Transaction Hash: 47291e0f6f1e689656179b19cf4d484c00e50412125f475e4272de50cb9de0de
Date: 3/18/2022 4:16:00 PM
Amount BTC: 5.3702
Sending Cluster: bc1qs5f3ta0rchzelsp5q8ptarr4sy9kfk8fkh36mc
Receiving Address: bc1qdk4s5kwh6uslvqy44ajksynjf2c564n6f6x2m3
Transaction Hash: 178a968fd048cf2325045a34eac330737d35d60a1effe82ff6f512e0c92f2b35
Date: 3/18/2022 4:26:00 PM
Amount BTC: 5.37

Sending Address: bc1qdk4s5kwh6uslvqy44ajksynjf2c564n6f6x2m3
Receiving Address: 1QJ8Ztg3JTq1Fsi7teU6b7Lr67Fai6Fcxo (TARGET BINANCE ACCOUNT 3)
Transaction Hash: 2a2155d714ee5d1802de62050377374a04b846b29504a7eef7f946b1cf222bcb

FIGURE 7

A visual depiction containing the transfers identified in Figure 7, are reflected in Attachment D.

36. Binance records indicate that the owner of deposit address 1QJ8Ztg3JTq1Fsi7teU6b7Lr67Fai6Fcxo is linked to Binance User ID 255304050. Binance records reveal that User ID 282843618 is owned by Gaurav Garg Suresh GARG. Binance verification records also reveal that GARG provided a United Arab Emirates Resident Identity Card. The nationality listed on the United Arab Emirates Resident Identity card is India. Additionally, IP address login information from Binance corroborate that User ID 255304050 is located in India.

37. Binance records reveal that GARG's Binance account with User ID 255304050 receives a large number of deposits, conducts a large number of withdrawals, and conducts a large number of trades. As of March 30, 2022, Binance records reveal that TARGET BINANCE ACCOUNT 3 held numerous virtual currencies to include, BNB ("BNB"), BitTorrent ("BTTC"), Sologenic ("SOLO"), Tokocrypto ("TKO"), Alien Worlds ("TLM"), Internet Computer ("ICP"), SHIBA INU ("SHIB"), Polkadot ("DOT"), APENFT ("NFT"), Bitcoin ("BTC"), Ethereum ("ETH"), Litecoin ("LTC"), TetherUS ("USDT"). OMG Network ("OMG"), TRON ("TRX"), ChainLink ("LINK"), Ripple ("XRP"), Cardano ("ADA"), FTX Token ("FTT"), Solana ("SOL"), Curve ("CRV"), Celer Network ("CELR"), Polygon ("MATIC"), and Dogecoin ("DOGE"). The total balance as of March 30, 2022 held in TARGET BINANCE ACCOUNT 3 converted to Bitcoin is approximately 20.67343905 BTC.

38. Binance records confirm that Binance account with User ID 255304050 received a deposit of 1.4 BTC outlined in Figure 5 as well as a deposit of 5.37 BTC outlined in Figure 6 and Figure 7. Binance records reveal that the deposit of 5.37 BTC to Binance account with User ID 255304050 is most recent deposit received by the account. Although funds have left the account since these two deposits, the value of the account has never gone below the combined value of the deposits corresponding to the victim's funds. Although the account contains more cryptocurrency (and cryptocurrencies other than bitcoin), I seek only to seize the amount of bitcoin to correspond with the bitcoin transferred from J.F.'s Coinbase account.

BACKGROUND ON CRYPTOCURRENCY

39. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[3] Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or

3 Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[4] Cryptocurrency is not illegal in the United States.

b. Bitcoin[5] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin

4 Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

5 Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems. Tether is a cryptocurrency that is hosted on the Ehtereum and and Bitcoin blockchain. Tether is a stablecoin, meaning it is linked to the U.S. dollar.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is a frequently used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions. As of

March 31, 2022, one bitcoin is worth approximately $45,000, though the value of bitcoin is generally much more volatile than that of fiat currencies.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[6] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that

6 A QR code is a matrix barcode that is a machine-readable optical label.

their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

f. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[7] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account.

g. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application;

7 *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

h. Another concept unique to cryptocurrencies is the concept of clustering. The term cluster refers to the group (subset) of cryptocurrency addresses that are all associated together and crated under the same cryptocurrency account.

i. Binance Capital Management Co., Ltd. ("BINANCE") is a Cryptocurrency exchange and custodian that allows users to buy, sell and store digital assets. They hold a Money Service Business Registration in the United States. Their registration shows an address of Level 3, Melita Court, Triq Giuseppe Cali, Ta'Xbiex XBX 1420, MALTA.

CONCLUSION

40. Based on all of the foregoing, as well as my training, education, and experience, I submit that there is probable cause to believe that the SUBJECT ASSETS constitute proceeds of violations of 18 U.S.C. 1343, and are therefore, subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C)

and criminal forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). Binance has further indicated, in response to an inquiry specific to this case, that it is willing to voluntarily freeze TARGET BINANCE ACCOUNT 1, TARGET BINANCE ACCOUNT 2, TARGET BINANCE ACCOUNT 3, and transfer cryptocurrency to the United States with a seizure warrant issued by a United States Magistrate Judge. On or about March 31, 2022, Binance froze TARGET BINANCE ACCOUNT 1, TARGET BINANCE ACCOUNT 2, and TARGET BINANCE ACCOUNT 3.

Respectfully submitted,

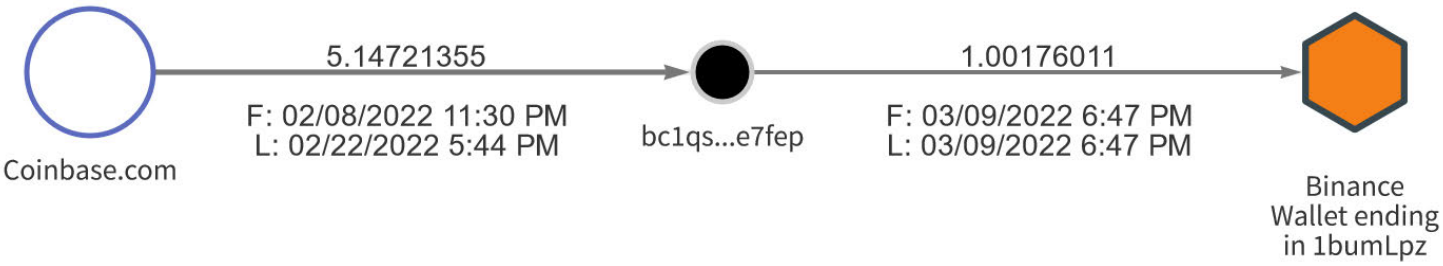
/s/ George Jasek
George Jasek III
Special Agent
United States Secret Service

The affiant appeared before me by telephonic conference on this date pursuant to Fed R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

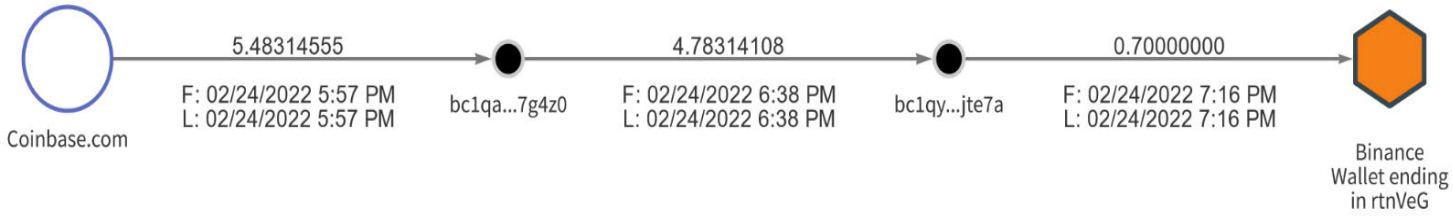
Date: **Apr 6, 2022**
Time: **11:50 AM, Apr 6, 2022**

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

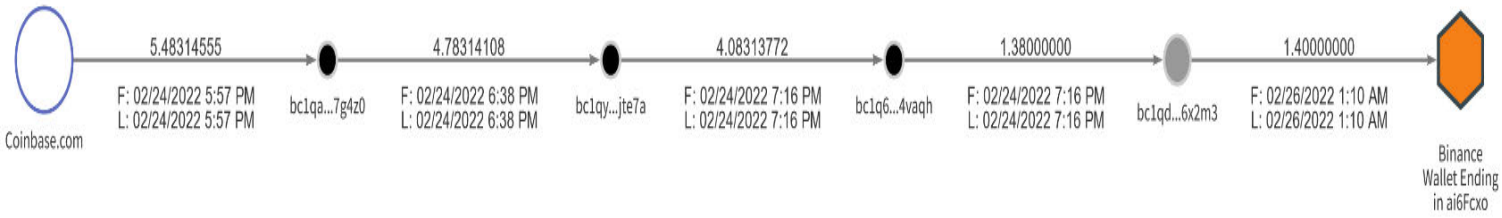
ATTACHMENT A



ATTACHMENT B



ATTACHMENT C



ATTACHMENT D